

EXHIBIT 1

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

NORTHWEST BIOTHERAPEUTICS, INC.,

Plaintiff,

v.

CANACCORD GENUITY LLC, CITADEL
SECURITIES LLC, G1 EXECUTION
SERVICES LLC, GTS SECURITIES LLC,
INSTINET LLC, LIME TRADING CORP.,
AND VIRTU AMERICAS LLC,

Defendants.

Case No. 1:22-cv-10185 (GHW) (GS)

[PROPOSED] ESI PROTOCOL

The ESI Protocol Order as set forth below is ORDERED:

This protocol describes the specifications for the production and use of electronically stored information, such as emails, electronic documents, hard copy documents (which will be converted to an appropriate electronic format as set forth below), text messages, instant messages and chat formats, audio and video files (including voicemail recordings), and any relevant structured data sources (“ESI”).

Nothing in this Order is intended to abrogate the applicability of Federal Rules of Civil Procedure 26, 34 and 37, Local Rules of the United States District Court for The Southern District of New York, the Court’s Individual Rules of Practice in Civil Cases, the Individual Practices in Civil Cases Before Magistrate Judge Gary Stein, or to obviate the parties’ respective rights and obligations under such Rules.

1. DEFINITIONS

Definitions will be construed according to the Federal Rules of Civil Procedure and The Sedona Conference® Glossary: E-Discovery & Digital Information Management (Fifth Edition), available at https://thesedonaconference.org/publication/The_Sedona_Conference_Glossary.

2. SEARCH METHODOLOGY

The parties will meet and confer regarding the search terms, custodians (subject to the provisions in Section 5, below), and date ranges (“Search Criteria”) that a Producing Party plans to use to identify ESI responsive to document requests if applicable. If a party chooses to utilize an automated or technology-assisted review (TAR) methodology to automatically code documents for responsiveness, that party must disclose the use of such review methodology to opposing counsel, including the name of the TAR application, and provide a protocol or other explanation reflecting how the automated or TAR technology will be used to identify relevant documents, particularly, how results will be validated.

3. DOCUMENT PROCESSING

3.1 Hidden Data. The parties will, during processing, ensure that documents display the following, where available:

- i. track changes (absent special circumstances, the TIFF images should show all track changes in markup form);
- ii. hidden columns or rows (noting that hidden columns or rows exist in native Excel files is sufficient);
- iii. hidden text or worksheets;
- iv. hidden slides in native PowerPoint presentations; and
- v. comments (these should be visible on the TIFF images of the documents).

3.2 Upon request by the receiving party, the producing party must produce native copies of any documents containing hidden data.

3.3 Compressed Files. Compression file types (e.g., .CAB, .GZ, .TAR, .Z, and .ZIP) shall be decompressed and extracted in a reiterative manner to ensure that a zip within a zip is decompressed into the lowest possible compression resulting in individual folders and/or files.

3.4 Exception Files. The Parties will use reasonable efforts and standard industry practices to address documents that present imaging or form production problems (including encrypted and/or protected files identified during the processing of ESI (“Exception Files”). A Party is not required in the first instance to produce Exception Files it has been unable to resolve through commercially reasonable efforts, except that, upon reasonable request, the producing Party will undertake reasonable efforts to locate passwords for specifically identified documents and to provide such passwords within thirty (30) calendar days of the request. Exception Files that are attached to produced documents will be produced as a Bates-stamped placeholder TIFF bearing a legend indicating the document is unable to be processed.

3.5 Password-Protected, Encrypted, or Proprietary-Software Files. With respect to any ESI items that are password-protected or encrypted within the scope of review, the producing Party will take reasonable steps to obtain identified passwords and remove such protection so that the documents can be reviewed and produced if appropriate. ESI that is likely to contain responsive information that cannot be reviewed because proprietary software is necessary to view the ESI will be disclosed to a requesting Party, and the Parties shall meet and confer regarding the next steps, if any, with respect to such ESI.

4. CELLPHONE, PERSONAL COMMUNICATIONS, AND STRUCTURED DATA

4.1 Cell Phones. If a Document Custodian (1) used a cell phone for purposes relevant to the Litigation and responsive to a Request for Production, and/or (2) used a cell phone to communicate regarding a subject relevant to the Litigation and responsive to a Request for Production, a producing Party will take reasonable steps to identify whether any unique, responsive ESI (including cell phone call logs, voicemails, voicemail logs, text messages and/or iMessages, chats [such as WhatsApp and Signal], notes, calendar items, emails, Word documents, photographs, audio recordings, and video recordings), if any, is located on any devices (including mobile phones, tablets, and computers) in the possession, custody, or control of the producing Party. Unless agreed otherwise, the following shall govern the identification of unique, responsive, and non-privileged communications for cellphone-based data for the agreed or ordered Document Custodians with respect to cellphones in the possession, custody, or control of the producing Party. Within a reasonable time period following the designation of a Document Custodian, whether by agreement or Court order, a producing Party is obligated to disclose if it takes the position that a Document Custodian possesses a cellphone that was used for purposes relevant to the Litigation but is not within the producing Party's possession, custody, or control; however, nothing in this ESI Protocol obligates a producing Party to subpoena a third-party to obtain the information described below.

- i. A producing Party shall use reasonable due diligence to ensure that reasonably available sources of data/applications on a cellphone (and related backups and archives, if those data sources/applications contain work-related information) are evaluated and considered as a potential source of data subject to discovery, including without limitation call and

voicemail logs, text messages, contacts, and image files (e.g., pictures and videos). A producing Party shall not be required to disclose any other cellphone-related information prior to any culling of cellphone data.

ii. For the categories below, a producing Party shall take reasonable steps to identify whether any unique, responsive ESI is located on any devices in the possession, custody, or control of the producing Party in accordance with the scope set forth below:

1. Cellphone Call and Voicemail Logs. The logs of any calls made/received to or from a Document Custodian, and logs of voicemails on a cellphone that the Document Custodian used for purposes relevant to this Litigation, if any, if the cellphone is in the possession, custody, or control of a producing Party.
2. Text Messages. All text messages and/or iMessages, or any other type of message or chat on a Document Custodian's cellphone device used for purposes relevant to the Litigation, if any, if the cellphone is in the possession, custody, or control of a producing Party, provided, however, that nothing herein shall obligate a Party to violate any applicable provision restricting employers from requiring an employee to disclose any user name or password for purposes of accessing an employee's personal account through the employee's personal electronic communications device. For text message chains that include responsive messages, the Parties will produce the text transcript for the day containing the responsive

message and can redact any portion of those chains that contain only non-relevant and non-responsive messages. To the extent a party encounters a difficulty with this production format, the Parties agree to meet and confer.

4.2 Social Media Data. If a Document Custodian (1) used social media for purposes relevant to the Litigation and responsive to a Request for Production, and/or (2) used that social media to communicate regarding a subject relevant to the Litigation and responsive to a Request for Production, then the requested communication(s) must be produced if it is reasonably accessible, in the producing Party's possession, custody, or control, and not withheld as privileged. Following the identification of a Document Custodian who used social media for purposes relevant to the Litigation, a producing Party is obligated to promptly disclose to a requesting Party if it believes the Document Custodian possesses social media materials that are not within the producing Party's possession, custody or control so that a requesting Party may issue a subpoena to that Document Custodian; however, nothing in this ESI Protocol obligates a producing Party to subpoena a third-party to obtain such social media materials or to take any actions that would violate any applicable provision restricting employers from requiring an employee to disclose any user name or password for purposes of accessing an employee's personal account through the employee's personal electronic communications device. If a requesting Party intends to issue a third-party subpoena directed at an employee of a producing Party concerning that employee's social media materials that are not in the producing Party's possession, custody or control, the requesting Party will provide notice of its intent to the producing Party prior to the service of the subpoena so that the Parties may meet and confer regarding the third-party subpoena. The

requesting Party may serve the subpoena 3 business days after the date of notice or at such earlier time agreed by the Parties.

4.3 Structured Data. To the extent a response to discovery requires production of discoverable ESI contained in a structured database, the Parties shall meet and confer in an attempt to agree upon a set of queries to be made for discoverable information and generate a report in a reasonably usable and exportable electronic file (e.g., Excel or CSV format) for review by the Requesting Party. Upon review of the report, the requesting Party may make reasonable requests for additional information to explain the database schema, codes, abbreviations, and different report formats or to request specific data from identified fields.

5. DOCUMENT SOURCE NEGOTIATIONS

5.1 Initial Document Custodians and Sources. Each Party will provide a list of proposed document custodians and non-custodial document sources (e.g., centralized document sources other than an individual document custodian's files) reflecting those employees or sources with information and/or documents responsive to Rule 34 Requests. The Parties shall be prepared to meet and confer regarding how discoverable information is stored and how it may be collected.

5.2 Additional Document Custodians or Sources. If, after the Parties identify initial document custodians, a requesting Party believes that additional document custodians or sources should be added, then the requesting Party shall advise the producing Party in writing of the proposed additional document custodians or sources and the basis for the request. If the Parties have not agreed on whether to add the document custodian or source within 30 days of the requesting Party's request, then the matter may be brought to the Court.

5.3 The Parties' discussion of proposed search terms, document custodians, or sources does not preclude a Party from requesting additional search terms, document custodians, or sources

pursuant to the terms of this ESI Protocol; nor does it preclude a Party from objecting to any such additional requests.

6. DATA CULLING

6.1 Duplicates. To the extent reasonably possible and accounting for any technical limitations of any Party's ESI, each Party may remove duplicate ESI, on a family basis, prior to producing documents. The parties may use MD5 or SHA-1 hash values to de-duplicate documents at the parent level. The Producing Party may de-duplicate documents within custodians and/or across custodians. With respect to such de-duplication, the Load File will contain a metadata field ("All Custodians") identifying all custodians who possessed exact copies of the document to the extent such information is readily available. The parties will not de-duplicate loose electronic documents against email attachments. The parties will not count a document containing handwritten notes, highlighting, or any other markings as a duplicate of a non-marked or annotated version of the same document.

6.2 Families. If any family member hits on a search term, the entire family must be included for review purposes. To the extent one or more documents in any family are responsive to any document request, the entire family must be produced, with the exception that privileged material may be redacted or withheld.

6.3 OCR. The parties must run optical character recognition ("OCR") conversion on non-searchable PDF files and other stand-alone files and email attachments that do not have searchable text in order to make them searchable before running the searches.

7. PRODUCTION

7.1 Media. Any production may be produced via FTPS or HTTPS site. Otherwise, the parties will deliver each production on a CD, DVD, or USB flash drive using overnight delivery,

or if a delivery is too large to fit on two CDs, DVDs, or USB flash drives, the production will be delivered via an external hard drive using overnight delivery. If any productions are made via physical storage hardware (including, but not limited to CDs, DVDs, USB flash drives, laptop computer, and/or external hard drives) such hardware shall be encrypted or password-protected prior to exchange. The production media should be labeled with:

- i. the Producing Party's name;
- ii. the case name and number;
- iii. the production volume; and
- iv. the Bates number range.

7.2 Production Format. Any files not produced in native form shall be produced as tagged image file format ("TIFF") images accompanied with an image load file, a data load file, and document-level searchable text.

- i. Image Requirements. A TIFF image converted from native file shall be produced as follows:
 1. All images shall be group 4 black and white 300 dpi TIFF files named according to Bates number (although a party may request a document be produced in color if required to understand its content);
 2. Requested color images will be produced in JPG format;
 3. Hidden content, tracked changes or edits, comments, and other similar information viewable within the native file shall also be imaged so that such content is viewable on the image;
 4. Bates numbers and confidentiality designations shall be branded to the images so that the numbers and designations print;

5. If a Bates number or set of Bates numbers is skipped in a production, the producing party will so note in a cover letter accompanying the production;
 6. Images shall be single page TIFFs (one TIFF file for each page); and
 7. Each TIFF image should be assigned a Bates number that is unique and maintains a constant length across the entire document production (i.e., padded to the same number of characters).
- ii. Data Load File Requirements. The parties will produce a Relativity-compatible .dat load file with standard Concordance delimiters with each production volume. The data load file will contain all fields listed on Appendix A with a header row describing each field. If a production volume contains trading or order data, the producing party shall produce such data with the relevant data fields maintained by the producing party in the ordinary course. The parties will also produce an Opticon-compatible .opt file to provide paths to individual Bates-numbered TIFF and JPG files.
1. The parties are not obligated to produce metadata from a document if metadata does not exist or if the metadata is not machine extractable, except that the parties will produce custodian metadata for hard-copy documents to the extent that a custodian is reasonably known or can be assigned.
- iii. Extracted and OCR Text Requirements. The parties will provide electronically extracted text for ESI. The parties will provide OCR text for

documents that do not contain electronically extractable text, for redacted documents, and for hard-copy documents.

1. The parties will provide document text as separate, document-level text files not embedded in the metadata load file; and
2. The parties will name each text file with the unique Bates number of the first page of the corresponding document, followed by the extension “txt.”

7.3 Native Production. The parties will produce data files (e.g., comma-separated or tab-separated files), spreadsheets (e.g., Excel), PowerPoint documents, and audio, video or multi-media files (e.g., text files with embedded images) in native form. The parties will replace the TIFF image with a document placeholder containing a unique Bates number and language sufficient to convey that the document was produced in native form, along with any applicable protective order designation. The text file will contain the extracted text of the native file. Additionally, PowerPoint documents shall be produced with single-page, 300 DPI TIFF/JPG images which display both the slide and speaker’s notes. Should any TIFF images not be legible, the parties will work together to provide native versions of such documents on a case-by-case basis.

- i. The parties will name each native file with the unique Bates number of the first page of the corresponding document, followed by the appropriate extension (“xls,” “csv,” or “ppt”, etc.);
- ii. The parties will provide a path to each native file in the data load file;

- iii. To the extent spreadsheets require redactions, they shall be redacted using a tool designed for redacting spreadsheets and produced in the form of a redacted “.xlsx.”
- iv. When redaction is necessary, a redacted full TIFF version may be produced instead; and
- v. The requirements of Paragraph 5.2(ii) apply equally to all documents produced in native format.

7.4 Hard-Copy Files. The parties agree to produce hard-copy documents in single-page, black-and-white Group IV TIFF image format named according to Bates number accompanied by document-level OCR text files. The parties also agree to provide load files linking the TIFFs with their associated text. The database load file should contain the following fields: “BatesBegin,” “BatesEnd,” “Confidentiality,” and “Custodian.” The documents should be logically unitized (i.e., contain correct document breaks: for instance, a five-page document consisting of a cover page and a four-page report should be unitized as a five-page document). The parties will scan hard-copy documents such that the images appear the same as the documents that are kept in the ordinary course of business. If a folder with hard copy documents is produced, the label of that folder should be scanned and produced along with the documents in the folder. The relationship among the documents in a folder or other grouping should be reflected in the use of a parent-child relationship and proper coding of the beginning and ending document and attachment fields to the extent reasonably practicable. If any original hard-copy document has notes affixed thereto or attachments, the parties will scan and produce copies of the notes or attachments in the same manner as other documents.

7.5 Other Files. The parties will meet and confer to discuss a suitable production format for any document types not addressed herein.

7.6 Bates Numbering. The Bates number and any confidentiality designation should be electronically branded on each produced TIFF image of ESI. For documents produced in native format, the Bates number and confidentiality designation should be electronically branded on the document placeholder.

8. CONFIDENTIALITY

Confidentiality of documents produced will be designated in accordance with the protective order entered in the above-captioned case on [Date], and any further protective orders or other orders entered in these proceedings.

9. PRIVILEGE

9.1 Privilege Log. The parties will provide a privilege log that complies with Rule 26 for any document withheld in whole or in part (i.e., redacted) based upon a claim of privilege. The privilege log will include the basis of the privilege claimed ((a) AC for Attorney/Client, (b) WP for Attorney Work Product, (c) CI for Common Interest; and/or (d) OTH for Other), a description sufficient to allow the receiving party to assess the privilege claim (although for descriptions, categorical privilege designations consistent with Local Rule 26.2(c) are permitted), and reasonable detail for each document based on the document's metadata.

9.2 All legal personnel will be indicated by an asterisk on the privilege log and the party that personnel represented, to the extent known or reasonably necessary to assess the privilege claim.

9.3 Communications exclusively between a party or its representative(s) on one side and its outside counsel in this action on the other created on or after December 1, 2022 need not be logged. Similarly, work product created on or after December 1, 2022 by counsel in this action, a consultant or other agent of counsel in the action, or a party at the direction of its counsel, need not be logged.

SO ORDERED.

Dated: New York, New York
_____, 2025

GARY STEIN

United States Magistrate Judge

Appendix A

Field Name	Description
BatesBegin	The first page of the document
BatesEnd	The last page of the document
AttachBegin	The first page/doc of the first parent of an attachment family. (e.g., ABC000001).
AttachEnd	The last page/doc of the last attachment. (e.g., ABC000019).
Custodian	Custodian name
All Custodians	All custodians of a globally deduplicated document separated by semicolons (e.g., Doe, John; Roe, Robert).
Tag - Confidentiality	The text demonstrating the confidential level of the document (e.g., Confidential, Highly Confidential, etc.)
EM - Subject	E-mail subject
EM - To	The values in the original “To” field for emails.
EM - From	The values in the original “From” field for emails.
EM - CC	The values in the original “CC” field for emails.
EM - BCC	The values in the original “BCC” field for emails.
EM – Date-Time Sent	Date and time the e-mail was sent in Eastern Standard Time
EM – Date-Time Received	Date and time the e-mail was received in Eastern Standard Time
File - Title	Title field value extracted from the metadata of the native file
EM – Meeting Start Date Time	Start date of calendar appointment. Format: MM/DD/YYYY HH:MM:SS AM/PM
EM – Meeting End Date Time	End date of calendar appointment. Format: MM/DD/YYYY HH:MM:SS AM/PM
File - Document Type	A reference to the application that created the file, for example “Word Document” or “Excel Spreadsheet”
File - File Name	Original file name
File - File Path	The path the original native file (excluding name and file extension)

Field Name	Description
File – All File Path	For globally and within custodian de-duplicated productions. Folder paths to this document's duplicates and the original path. Each path will contain the associated custodian.
File - File Size	File size of the native file in bytes.
File – Date-Time Created	Date and time the file was created (not applicable to e-mails that were sent or received)
File – Date-Time Modified	Date and time the file was last modified (not applicable to e-mails that were sent or received)
File – Date-Time Printed	Date and time the file was last printed (not applicable to e-mails that were sent or received)
Extracted Text Path	File path to the extracted text/OCR file, or the extracted/OCR file link (e.g. ABC001\Text\001\ABC000001.txt)
Native File Path	File path to the native file, or the native file link (e.g., ABC001\Native\001\ABC000001.xls)
MD5Hash	Unique "fingerprint" that exists for every document. This identifier is used for identification of exact duplicate documents.
Social media / cell phones – Participants	The participants of the text/chat, either by name or phone number (or both).
Social media / cell phones – Type	The type of message (e.g., text, chat, or other).
Social media / cell phones – Text/Chat Group	Allows grouping of all chats/texts from the same string together.
Pages	The number of Bates stamped pages of the document.
HiddenContent	Denotes presence of Tracked Changes/Hidden Content/Embedded Objects in item(s).